NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA, Plaintiff, v. ROGER DURONIO, Defendant.	Criminal Action No. 02-933 (JAG) **OPINION**

GREENAWAY, JR., U.S.D.J.

This matter comes before this Court on Defendant Roger Duronio's ("Defendant") motion to dismiss the indictment. Defendant Duronio is charged in a multiple count indictment with, inter alia, securities fraud, mail fraud, and computer fraud. Defendant argues that the Government violated its obligations, pursuant to Brady v. Maryland, 373 U.S. 83 (1963), because evidence that should have been produced to Defendant was destroyed. Specifically, Defendant argues that post-indictment his former employer, UBS/Paine Webber ("UBS"), destroyed another UBS employee's computer ("CR computer"), an "infected but unaffected computer,"[1] and a host computer ("sa.drm computer").[2] Defendant avers that his right to due process has been adversely

[1] The "infected but unaffected computer" contained logic bomb code, but its files were not deleted. (Def.'s Reply Br. 7.) UBS put this computer back into use, but it was reconfigured, thus deleting its files. (Id.) Back-up tapes have been located for this computer; however, back-up tapes are not the equivalent of a mirror image of the CR computer. (Id. at 8.) The back-up tapes do not exactly duplicate the state of the computer at the time of the logic bomb. See infra n.7.

[2] In December 2005, the sa.drm computer was located and is no longer at issue. (2 Tr. 4:8-11 ["2 Tr." refers to the transcript of proceedings held on February 17, 2006].)

affected.[3] At oral arguments, Defendant limited the motion to the CR computer, classifying the issue as the "most easily understandable" and the "most offensive." (1 Tr. 83:14-16; 2 Tr. 3:24-5:6.)[4]

BACKGROUND

On June 28, 1999, Roger Duronio began working at UBS as a systems administrator. (Gov't's Br. 4.) Prior to accepting this position, Mr. Duronio had worked over twenty years as a systems administrator for numerous companies. (Def.'s Br. 2.) At UBS, Mr. Duronio was responsible for maintaining and troubleshooting the computer environments, operating system software, and support software. He had full and complete access to the computer systems, both from the office and his home. (Id. at 2-3). Mr. Duronio resigned from his position with UBS on February 22, 2002. (Gov't's Br. 4.)

On March 4, 2002, a logic bomb[5] began destroying files on over one thousand UBS computer servers nationwide, resulting in system failures in both the headquarters of UBS in New Jersey and four hundred retail branches nationwide ("March 4th Incident"). (Id. at 3.) UBS spent over three million dollars to identify the source of the problem and repair the damage. Additionally, UBS suffered economic harm to its business due to the interruption of work

[3] The Due Process Clause of the Fifth Amendment of the Constitution provides that "[n]o person shall . . . be denied life, liberty, or property, without due process of law." U.S. CONST. amend. V.

[4] "1 Tr." refers to the transcript of the proceedings held on December 13, 2005.

[5] A logic bomb is similar to a computer virus, except that its execution is delayed pending satisfaction of certain criteria, such as a date or time. This logic bomb was set to execute at 9:30 a.m. on Mondays in March, April, and May of 2002, and was instructed to delete all files from computers on which it operated. (Gov't's Br. 5 n.1.)

activity. (Id.) By March 6, 2002, UBS contracted with @Stake[6] to perform a digital forensic investigation on affected computers which had been damaged by the attack and whose files had been deleted. (Id.) After @Stake confirmed that the system failure was deliberately caused, UBS contacted criminal authorities on March 18, 2002 to report the March 4th Incident. A criminal investigation, conducted by the Secret Service, followed. (Id.)

On March 21, 2002, government agents searched Mr. Duronio's residence, finding evidence that they believed connected him with the creation and execution of the logic bomb. (Id. at 5). Two months later, the United States Attorney's Office met with Mr. Duronio and presented him with the evidence against him. (Id.)

On July 23, 2002, the Secret Service interviewed two UBS employees, Charles Richardson ("CR") and William "Rob" Robertson ("RR"). (Id. at 7.) The interview focused on CR's and RR's knowledge of Duronio's involvement in the March 4th Incident. CR and RR were told that they were not subjects of the investigation. (Id.) Soon after, UBS began their own investigation of CR and RR, and asked @Stake to evaluate whether they may have been involved in the logic bomb attack. (Id.) CR and RR's computers were removed from their offices by @Stake for evaluation. In accordance with @Stake's policy, @Stake also made mirror images[7] for examination. (2 Tr. 49:3-5.) CR's computer was found to contain similarly named code as

[6] @Stake is an independent company hired by other companies to assist in solving and repairing computer system crises and investigating the source of the problem. (Gov't's Br. 3.)

[7] A mirror image is a duplication of a computer's hard drive in a specific state. A computer forensics company, such as @Stake, can then work with the mirror image to determine the source of the computer problems, instead of working with the actual computer. In this case, the mirror image of the computers was taken after the March 4th Incident. (2 Tr. 48:21-49:20.) A forensically secured mirror image is different than a back-up tape, which is usually taken during the ordinary course of business. For investigating computer problems, a mirror image is more useful. (Id. 83:8-25.)

that of the logic bomb files.[8] (Gov't's Br. 31.) However, @Stake "concluded that it was 'unlikely [that] CR and RR were directly involved in any malicious activity against UBS,'" (Id. at 7 (quoting @Stake report)) and that the actual logic bomb files did not exist on the CR and RR computers. (Gov't's Br. 31.) CR and RR were placed on administrative leave and ultimately fired.[9] (Id. at 8.)

Though UBS contacted criminal authorities on March 18, 2002, the United States Attorney's Office was not aware of UBS's investigation of CR until over two years later. (Aff. of Robert Bunker, Dec. 13, 2005 ¶ 7.) As of January 21, 2005, UBS denied awareness of any other system users who were investigated besides Duronio. (Aff. Lin Solomon ¶ 9.) On October 13, 2005, Defendant served a Rule 17(c) subpoena on UBS demanding an unredacted @Stake report and various security documents. (Id. at ¶ 21.) On October 31, 2005, UBS revealed that @Stake conducted an investigation of other UBS employees, including CR. (Id. at ¶ 22.) This investigation had not previously been revealed to either the government or Defendant. (Id.) In November 2005, Defendant requested an opportunity to examine CR's computer, but the government informed Defendant that CR's computer had been reconfigured[10] by UBS for use by another user, and CR's computer files no longer existed. (Def.'s Reply Br. 7.)

@Stake was subsequently acquired by the Symantec Corporation and @Stake's forensic laboratories were destroyed in 2003. (Third Aff. Lin Solomon, Ex. B; 2 Tr. 49:6) Counsel for

---

[8] The Defense contends that this signifies that the logic bomb could have been created on the CR computer. (Def.'s Br. 5.)

[9] Both CR and RR were informed that they were not targets of the criminal investigation, merely that they had contact with the individual who was the target. (Gov't's Br. 8.)

[10] Reconfiguring a computer wipes a computer clean, "like cleaning a chalkboard." (2 Tr. 49:19-20.) After a UBS employee is dismissed, their computer is reconfigured for use by another employee, removing "all that stuff on that hard drive that the previous employee was using." (2 Tr. 47:3-4.)

the Symantec Corporation informed Defendant that the mirror image of CR's computer, taken by @Stake in July or August of 2002, could not be located. (2 Tr. 49:6-8.)

STANDARD OF REVIEW

Defendant claims that the reconfiguration of CR's computer by UBS and the destruction of the mirror image by @Stake or Symantec on an unknown date (but prior to November 2005) constitutes a Brady violation. Specifically, the destruction of CR's computer precludes the Defendant from proving that the source of the logic bomb was other than his computer. Thus, Defendant argues, CR's computer could have contained, if it had been retained, exculpatory evidence. More importantly, in Brady, the Supreme Court held that "the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution." Brady, 373 U.S. at 87.

To prove a Brady violation, a defendant must show that: 1) evidence was suppressed by the government; 2) this evidence was favorable to the defense; and 3) the evidence was material to guilt or punishment. United States v. Pellulo, 399 F.3d 197, 209 (3d Cir. 2005) (citing United States v. Dixon, 132 F.3d 192, 199 (5th Cir.1997)). A prosecutor's duty to disclose material evidence reaches beyond merely evidence in the government's possession. Kyles v. Whitley, 514 U.S. 419, 437 (1995); see also United States v. Pedermo, 929 F.2d 967, 970 (3d Cir. 1991) (non-disclosure of prosecution witness's criminal background information constituted a Brady violation although information was not in prosecution's possession).

To satisfy the first Brady factor, Defendant argues that UBS's and @Stake's alleged suppression and destruction of the CR computer should be imputed to the government. Recently, in United States v. Risha, No. 04-4667, 2006 WL 1061961 (3d Cir. Apr. 24, 2006), the United

States Court of Appeals for the Third Circuit set out factors to determine whether a state agency's knowledge can be imputed to the federal government. In Risha, a federal prosecutor's key witness received a favorable plea agreement in an unrelated state prosecution pending against him in return for testifying in the federal case, a fact which was unknown to the federal prosecutor. Id. at *1. The Court of Appeals was faced with the question of whether, because of a close involvement between the federal prosecution and state agents, it could impute knowledge of the plea bargain to the federal prosecutors. Id. The questions the Risha Court developed to ask when determining whether to impute knowledge to the federal government are:

> 1) whether the party with knowledge of the information is acting on the government's "behalf" or is under its "control"; 2) the extent to which [the party with knowledge] and [the] federal government[] are part of a "team," are participating in a "joint investigation" or are sharing resources; and 3) whether the entity charged with constructive possession has "ready access" to the evidence.

Risha, 2006 WL 1061961 at *6.

In Risha, the Third Circuit thought it likely that impeachment information was readily available to the prosecution and that there was a close working relationship between the federal prosecution and state agents. Id. at *6. However, the Court of Appeals remanded so that the District Court could make the fact driven determination of whether the federal prosecutor should have known of Brady material. Id. at *8.

DISCUSSION

1. Neither UBS Nor @Stake Is Acting on the Government's Behalf, Nor Are They Part of a Team or Joint Investigation.

The first two Risha factors examine whether the entity charged with knowledge of the information or evidence was acting under the government's control or on its behalf, and whether the entity and the government participated in a joint investigation or a team effort. Id. at *6. To determine whether an entity is acting on the government's behalf, courts have looked to factors

such as whether the entity assists the prosecution before and during trial, and whether the entity conducts interrelated or independent investigations from the government. See Risha, 2006 WL 1061961 at *6; Moreno-Morales v. United States, 334 F.3d 140, 146 (1st Cir. 2003) (Puerto Rico Senate conducted separate investigation from the federal authorities and was not "working on behalf" of the federal government). Additionally, courts have found team efforts and joint investigations where the entity and the federal government "pooled their investigative energies to a considerable extent" and the "entire effort was marked by [a] spirit of cooperation." United States v. Antone, 603 F.2d 566, 569 (5th Cir. 1979). However, where an entity purposely withholds information from the government, courts have been reluctant to find a team effort. See United States v. Joselyn, 206 F.3d 144, 153 (1st Cir. 2000).

In the instant case, the evidence was destroyed by @Stake, or their successor Symantec, without the knowledge of UBS, therefore UBS cannot be the "party with knowledge" referred to in Risha, 2006 WL 1061961 at *6. Even if @Stake were an agent of UBS, UBS was not acting on the government's behalf nor participating in a joint investigation. @Stake was hired by UBS and performed the first investigation of UBS's computers, before the government was even contacted. Furthermore, even though @Stake shared some of its findings with the government, the government contracted with their own expert, Foundstone, to conduct an additional investigation along with the Secret Service. (2 Tr. 25:21.)

Additionally, the government does not appear to have shared its findings with @Stake as they might have done under a "spirit of cooperation." Antone, 603 F.2d at 569. Furthermore, UBS and the government had differing interests regarding investigations of the March 4th Incident. After reporting the March 4th Incident to the government, UBS's interests refocused on preventing similar incidents by other employees and not disclosing network information or

computer security vulnerabilities (Gov't's Br. 28-29), while the government focused on prosecuting Mr. Duronio. See Joselyn, 206 F.3d 144, 153 (where disparate interests precluded attribution of knowledge). Finally, UBS clearly was not cooperating with the government or acting within its control as UBS's counsel failed to disclose to the government, for two years, that CR was the subject of an internal investigation.

2. The Government Did Not Have "Ready Access" to the CR Evidence.

The third Risha factor examines whether the prosecution has ready and available access to the information and evidence. Risha, 2006 WL 1061961 at *6. The government, if working jointly with a third party, would logically have ready access to the information and evidence held by the third party. The government has ready access to information if a "simple inquiry" would have yielded the specific information or evidence. Risha, 2006 WL 1061961 at *6. Similarly, if only "minimal steps" are "necessary to acquire" the evidence at issue, the government shall be found to have ready access to it. United States v. Joseph, 996 F.2d 36, 40 (3d Cir. 1993). The government could not merely have inquired as to the location of the CR computer or its mirror image, as it did not know of UBS's investigation of CR until after the destruction and reconfiguration of the CR computer. In fact, the government did inquire as to any investigations of other employees, but UBS denied any knowledge thereof. (Aff. Lin Solomon ¶ 9.) Thus, more than minimal steps would have been necessary to acquire the information regarding the CR investigation and thereafter any relevant computer evidence. Here, the government did not have ready access to the CR information or evidence, and knowledge thereof cannot be imputed to it.

Defendant has failed to demonstrate that: 1) UBS or @ Stake was acting on behalf of the government or under government control; 2) UBS or @Stake and the government participated in a joint investigation; and 3) the government had ready and available access to the information

and evidence.

CONCLUSION

Defendant has not shown that the knowledge of either UBS or @Stake should be imputed to the government. Neither UBS's nor @Stake's knowledge can be attributed to the government. Defendant has failed to prove that evidence was suppressed by the government, as required before a Brady violation may be shown. Thus, Defendant has failed to show a violation of his right to due process,[11] and his motion to dismiss the indictment shall be denied.

Dated: May 23, 2006

S/Joseph A. Greenaway, Jr.
JOSEPH A. GREENAWAY, JR., U.S.D.J.

[11] Even if UBS's and @Stake's knowledge is attributed to the government, Defendant still has not demonstrated a due process violation. @Stake analyzed the CR computer data and determined that there were no alternative theories of liability which did not involve Mr. Duronio. (2. Tr. 25:5-10.) Thus, the CR evidence is not apparently exculpatory because "the exculpatory value of the evidence must be apparent '*before* the evidence [is] destroyed.'" Arizona v. Youngblood, 488 U.S. 51, 56 n.1 (1988) (citing California v. Trombetta, 467 U.S. 479, 489 (1984)). The CR evidence is at most potentially exculpatory, thus bad faith on the part of the government must be shown to constitute a due process violation for destruction of evidence. Youngblood, 488 U.S. at 57-58. The "destruction of evidence in accordance with an established procedure precludes a finding of bad faith absent other compelling evidence." United States v. Deaner, 1 F.3d 192, 201 (3d Cir. 1993); see also Trombetta, 467 U.S. at 488 (failure to preserve breath tests is not a due process violation because the police were acting in good faith and in accord with their normal practice when they destroyed the tests) (quotation omitted); United States v. Boyd, 961 F.2d 434, 437 (3d Cir.), cert. denied, 506 U.S. 881 (1992) (destruction of a urine sample after two months in accordance with independent laboratory policy is not bad faith). Furthermore, mere negligence in failing to preserve evidence does not constitute bad faith. Youngblood, 488 U.S. at 58; United States v. Seibart, 148 F. Supp. 2d 559 (E.D. Pa. 2001). The CR computer was reconfigured in accordance with UBS's policy of reconfiguring former employees' computers for use by new employees, and the mirror image was lost or destroyed by Symantec when they acquired @Stake. (2 Tr. 48:3-4; 49:6-8.) As bad faith destruction of potentially exculpatory evidence has not been shown, there is no due process violation.